Amendments to the Drawings:

Figure 1 is amended to show multiple users (105) with lines connecting the multiple users (105) with shared device (110). Figure 1 is also amended to delete reference to the second computer, originally labeled as reference numeral 105, which had been connected to the network (115). Support for the amendments to Figure 1 can be found in the specification on page 8, lines 11-16.

Figure 2 is amended to show multiple users (105) with lines connecting the multiple users (105) with SmartCard (200). Figure 2 is also amended to environment (230), along with a corresponding bracket. Support for the amendments to Figure 2 can be found in the specification on page 8, line 11 through page 9, line 9.

Attachment: Replacement Sheets(2)
Annotated Sheets(2) Showing Changes

REMARKS/ARGUMENTS

Amendments are made to the specification and to the figures, as provided in the corresponding sections of this response. Support for the amendments to the specification and to the figures is provided with each described amendment in the corresponding sections of this response.

Claims 1-12 are pending in the present application. Claims 1-12 are amended and claims 13-18 are added. Support for the amendments can be found in the originally filed claims and in the specification on page 9, line 16 through page 10, line 22. Support for the new claims can be found in the specification on page 11, line 21 through page 12, line 22. Reconsideration of the claims is respectfully requested.

I. Objection to the Specification

The examiner objects to the specification. Applicants have amended the specification accordingly to delete objected-to subject matter and to provide the required support for the figures. No amendments to the specification add new matter. Therefore, this objection is overcome. Additionally, the text of the original abstract is added to the specification by way of amendment in this response.

II. Objection to the Abstract

The examiner objects to the abstract. Applicants have deleted the original abstract and provided a new abstract that is in compliance with the requirements of MPEP §608.01(b). The replacement abstract does not add new matter. Therefore, this objection is overcome.

III. Objection to the Drawings

The examiner objects to the drawings. Applicants amended the drawings accordingly. No amendments to the drawings add new matter. Therefore, this objection is overcome.

IV. 35 U.S.C. §101, Asserted Non-Statutory Subject Matter

The examiner rejects claim 12 as directed towards non-statutory subject matter. Applicants have amended claim 12 accordingly to recite that the computer program is on a tangible medium. This feature allows the computer program's functionality to be realized. Therefore, this rejection is overcome.

V. 35 U.S.C. §102, Asserted Anticipation

The examiner rejects claims 1 and 3-12 as anticipated by *Lambert et al.*, Method for Controlling Access to Electronically Provided Services and System for Implementing Such Method, U.S. Patent 6,282,649 (August 28, 2001) (hereinafter "*Lambert*"). This rejection is respectfully traversed.

Regarding claim 1, the examiner states that:

> **As to claim 1**, *Lambert* discloses a data processing system for controlling access of at least one user to stored data (column 2, lines 2-3, "a data processing system...for controlling user access to data," column 4, line 6, "retail till or automatic teller terminal," see *also* Figure 1) comprising: means, responsive to a request from the user to access a set of the stored data, for authenticating the user (column 2, lines 11-12, 33-35 "If the user key represents the required level of access authority an access key is generated from the user key for accessing that data or service...a user presents a token and inputs personal data (for example a personal identification number or PIN, input via a keypad)." Figure 1, and column 4, lines 22-25 "Partial key data (5) is read from a card presented by a user and supplied to a key generator (7). Personalized data such as a personal identification number (PIN) or biometric data is obtained from the user by a reader (8)"); means, responsive to successful authentication, for decrypting an encrypted data structure associated with the user (column 4, line 16 "A decryption service module"), wherein the data structure comprises data associated with the set (column 2, lines 1-28 (encrypted data structure contains data (applets) associated with the user via authority levels, and the data structure comprises data associated with the set (the applets). Also, column 4, lines 7-10 "An application store is provided to retain in encrypted form those applications which the terminal may be called on to perform, according to the authority of users requesting the application."); and means, responsive to successful decryption, for accessing the set (column 2 , lines 38-39 "controlling user access to data or services via a computer system," column 4, lines 5-6 "retail till or automatic teller terminal," see *also* Figure 1, and column 5 , line 29 "a checkout terminal," *see also* Figure 4).

Office Action dated October 10, 2006, pp. 5-6.

A prior art reference anticipates the claimed invention under 35 U.S.C. §102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). In this case each and every feature of the presently claimed invention is not identically shown in the cited reference, arranged as they are in the claims.

Claim 1 as amended is as follows:

> 1. (Currently Amended) A data processing system for controlling access of at least one user to stored data, the data processing system comprising:
>
> means, responsive to a request from the user to access a set of the stored data that is available to the at least one user, for authenticating the user;

means, responsive to successful authentication, for decrypting a user specific table associated with the user, wherein the user specific table identifies the set; and

means, responsive to successful decryption, for accessing the set.

Lambert does not anticipate claim 1 as amended because *Lambert* does not teach the claimed feature of, "means, responsive to successful authentication, for decrypting *a user specific table* associated with the user, *wherein the user specific table identifies the set*," as in claim 1. Instead, *Lambert* describes improving the security of stored data and applications by an access control system in which user keys for accessing the stored data/services are representative of the user's level of authority, such that there is no need to maintain a separate lookup table of user authority levels. These features remove a potential security exposure from the system. The user keys in *Lambert* are hierarchical, including data for generating a plurality of different access keys for each of a plurality of different access levels. The access keys in *Lambert* may be decryption keys for encrypted data or application programs.

However, *Lambert* is devoid of disclosure regarding a user specific table associated with the user, wherein the user specific table identifies the set of the stored data that is available to the at least one user, as in claim 1. Because *Lambert* does not teach this claimed feature, *Lambert* does not anticipate claim 1 under the standards of *In re Lowry*.

Nevertheless, *Lambert* does teach the following:

> A problem arises when seeking to control access to application program modules where a number of different users are required to be allowed to access different sets of application modules. For example, in a retail environment, it may be desirable for all till operators to run certain applets associated with sales whereas only the store manager can access other applets associated with stock control or payroll. The conventional approach to this problem is for a computer LOG ON procedure to include identification of the user from user input data (and optionally additional data held on a token such as a SmartCard). A table lookup process then scans a static list to determine the access authority of the user, and the user is given access to certain applications according to their determined authority level.

Lambert, col. 1, ll. 48-61.

This portion of *Lambert* teaches that a table lookup process scans a static list to determine the access authority of the user. The user is then given access to certain applications according to their determined authority level. However, this portion of *Lambert* does not teach the claimed feature of, "means, responsive to successful authentication, for decrypting *a user specific table* associated with the user, *wherein the user specific table identifies the set*," as in claim 1. Instead, a table lookup process scans a single *static list* to determine the access authority of the user. Thus, even assuming, *arguendo*,

that the "table lookup process" involves looking up user specific tables, a point Applicants do not concede, the user specific table does not identify the set of data to which the user has access. Instead, the *authority level* of the key determines the access, not the user specific table.

Additionally, the "table lookup process" in *Lambert* is not equivalent to the "user specific table" in claim 1. Instead, the table lookup process describes a process by which a single static list is scanned. The single static list is not the same as a user specific table. Similarly, a user specific table is not used to scan the list. Instead, "a table lookup process" is used to scan the static list, though *Lambert* does not describe the details of how the table lookup process operates.

Thus, again, *Lambert* does not teach the claimed feature of, "means, responsive to successful authentication, for decrypting *a user specific table* associated with the user, *wherein the user specific table identifies the set*," as in claim 1. Therefore, *Lambert* does not anticipate claim 1.

Claims 1, and 3-18 all contain features similar to those presented in claim 1 as amended. Therefore, *Lambert* does not anticipate these claims at least for the reasons presented above.

Additionally, *Lambert* does not teach all of the features of the dependent claims. For example, *Lambert* does not teach, "wherein the data processing system includes a corresponding additional user specific table for each additional user of the at least one user, wherein the means for decrypting also comprises means for attempting to decrypt, in turn, each of the corresponding additional user specific tables as well as the user specific table until a successful decryption occurs," as in new claims 13, 15, and 17. Similarly, *Lambert* does not teach, "wherein means for authenticating the user further comprises means for pointing the user to an unencrypted table that stores a corresponding location of each user specific table for each user of the at least one user," as in new claims 14, 16, and 18. Therefore, the anticipation rejection has been overcome.

VI. 35 U.S.C. §103, Asserted Obviousness

The examiner rejects claim 2 as obvious over *Lambert* in view of *Bartocci et al.*, Generalized Directory Data Model, European Patent Application Publication 0 204 994 A2 (December 17, 1986) (hereinafter "*Bartocci*"). This rejection is respectfully traversed.

The examiner states that:

> **As to claim 2,** Lambert fails to teach data associated with the set comprising data associated with the location of the set. Bartocci teaches data associated with the set comprising data associated with the location of the set (column 7, lines 1-4 "User Data Pointer [--] This is location dependent address information used to direct access at this DSU [Directory Service Unit] to user Page 9 data" see *also* Figure 6).
>
> Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lambert by the user data pointer for data

> associated with the set to include the location of the set as taught by Bartocci in order to enable remote data management.

Office Action dated October 10, 2006, pp. 10-11.

The Examiner bears the burden of establishing a *prima facie* case of obviousness based on prior art when rejecting claims under 35 U.S.C. §103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). A *prima facie* case of obviousness is established when the teachings of the prior art itself suggest the claimed subject matter to a person of ordinary skill in the art. *In re Bell*, 991 F.2d 781, 783, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). For an invention to be *prima facie* obvious, the prior art must teach or suggest all claim limitations. *In re Royka,* 490 F.2d 981, 180 USPQ 580 (CCPA 1974). In the case at hand, the cited references when considered as a whole do not teach or suggest all of the limitations of the claims, arranged as they are in the claims.

In the case at hand, the proposed combination of *Lambert* and *Bartocci*, when considered together as a whole, does not teach or suggest the claimed feature of, "means, responsive to successful authentication, for decrypting a user specific table associated with the user, wherein the user specific table identifies the set," as in claim 1 from which claim 2 depends. As shown above, *Lambert* does not teach this claimed feature. Because *Lambert* is devoid of disclosure in this regard, *Lambert* also does not suggest this claimed feature.

Additionally, *Bartocci* does not teach this claimed feature. Bartoccci discloses a directory data model for use in storing mappings of information. *Bartocci* does disclose a user data component of the described database. *Bartocci* describes the user data component as follows:

> Fig. 5 depicts the user data component. This collection of directory data elements (a member of the directory database) is referenced by a named directory identifier (ID). In this model, user data is comprised of data elements, each having multiple fields of arbitrary length. The data element is segmented into fields to facilitate use of defaults and reference of fields by means of their specified field names through commands at the user protocol boundary.

Bartocci, col. 6, ll. 7-17.

Bartocci also describes a user data descriptor component of the described database. *Bartocci* describes the user data descriptor component as follows:

> The user data descriptor (Fig. 6) describes user data and those access controls particular to this member of the directory database. The scope of access control is that of the entire user data object rather than that of the data element. The user data descriptor includes the directory type ID, which names the directory database, a user data pointer, an indication of the number of elements which comprise this member, format data, and access control.

Bartocci, col. 6, ll. 39-48.

From these descriptions, the user data component in *Bartocci* is a collection of directory data elements referenced by a named identifier. The user data descriptor in *Bartocci* describes user data and those access controls particular to the member of the directory database. However, the scope of access control is that of the entire user data object, rather than that of the data element. In contrast, claim 2, through claim 1, provides for, "means, responsive to successful authentication, for decrypting *a user specific table associated with the user, wherein the user specific table identifies the set.*" This feature is not equivalent to *Bartocci*'s teaching that the scope of access control is that of the entire user data object, because the user data object contains reference to multiple users. Thus, *Bartocci* does not describe a user specific table associated with the user, wherein the user specific table identifies the set of data to which the user has access, as claimed.

Moreover, *Bartocci* does not suggest this claimed feature because *Bartocci* is devoid of disclosure in this regard. Because neither *Lambert* nor *Bartocci* teach or suggest the features of claim 2, through claim 1, the proposed combination, when considered as a whole, does not teach or suggest all of the features of claim 2. Accordingly, under the standards of *In re Royka*, no *prima facie* obviousness rejection can be made against claim 2 using a combination of these references. Therefore, the obviousness rejection is overcome.

VII. Conclusion

The subject application is patentable over the cited references and should now be in condition for allowance. The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: January 10, 2007

Respectfully submitted,

/Theodore D. Fay III/

Theodore D. Fay III
Reg. No. 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants

10/698,174

ANNOTATED SHEET

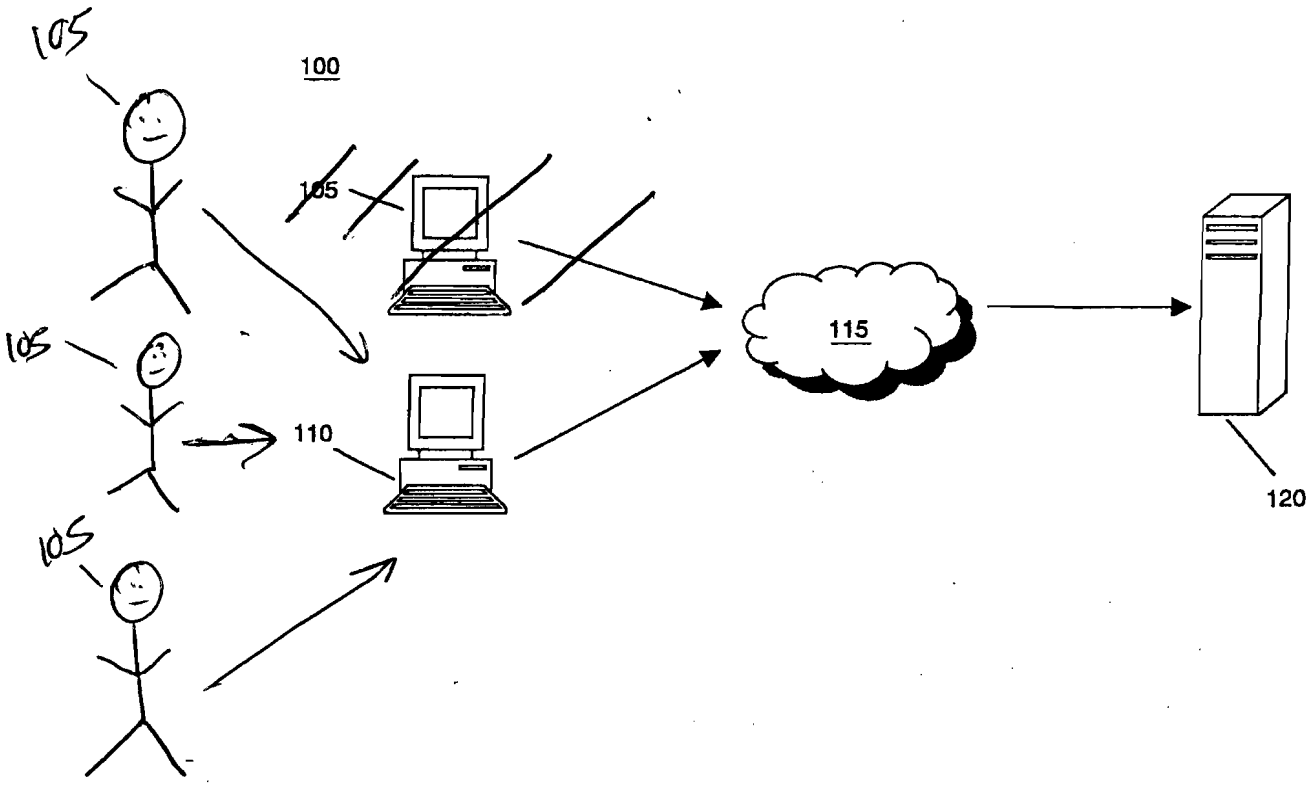

FIG. 1

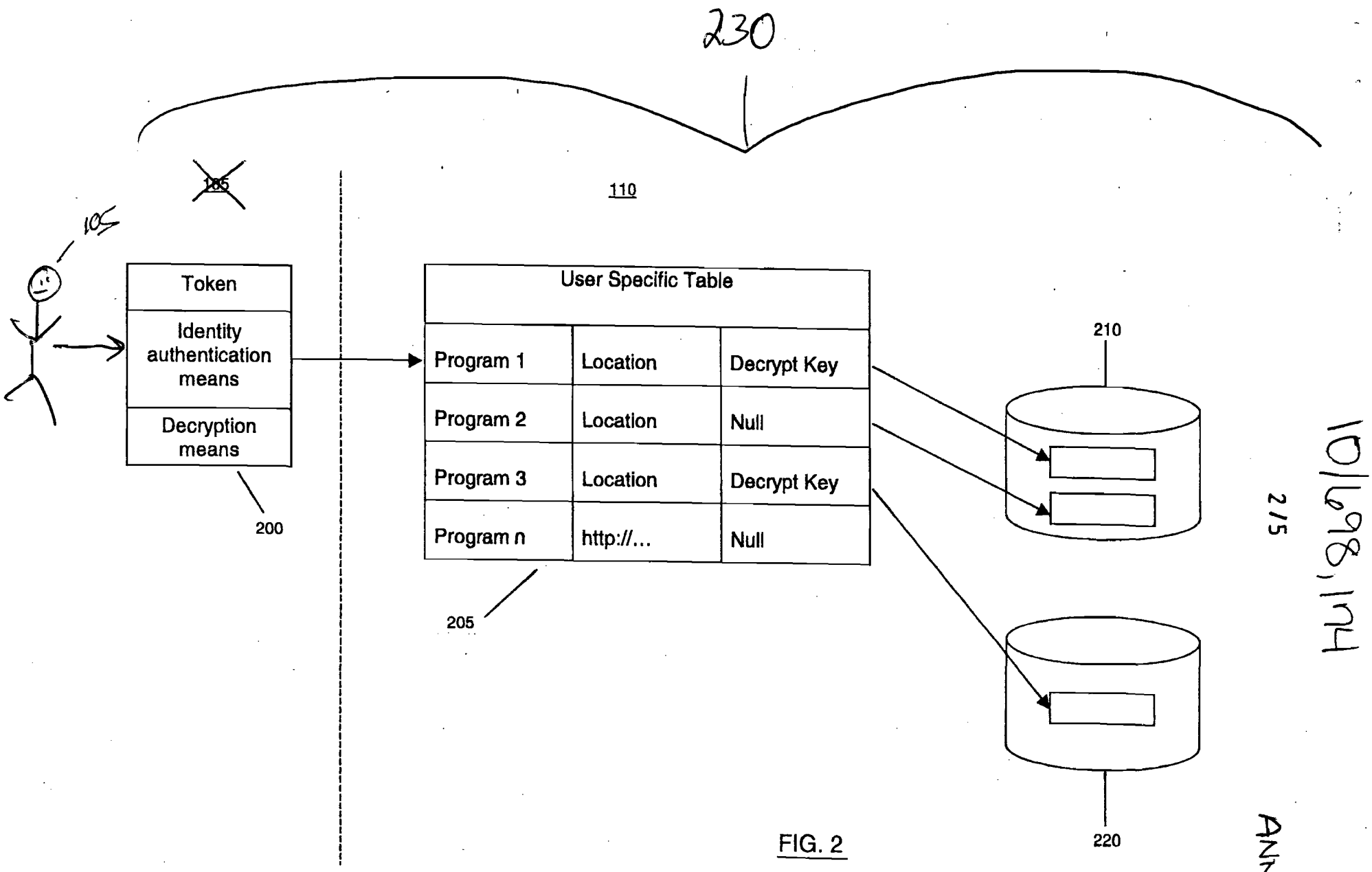

FIG. 2